CLAIMS

Claims 1-19 (canceled)

20. (Currently Amended) A method, comprising:

______~~for~~ enabling integrity checking of a software module to be used in a mobile communication terminal, said terminal capable of communicating in a mobile communication system, said software module already stored on a removable memory unit connected to the terminal and ready for use except, before allowing the software module to take control of the terminal, the terminal communicates via the mobile communication system with a software provider, said communication ~~including~~ including:

______transmitting by said terminal of identifying information concerning said terminal and said memory unit to said software ~~provider~~ provider,

______~~and~~ receiving by said terminal a digitally signed data block comprising a reference value for use during integrity checking of said software ~~module~~ module, and

______allowing the software module to take control of the terminal only if the integrity of the software module properly checks.

21. (previously presented) The method of claim 20, comprising:

hashing the software module, resulting in a first hash value, wherein said transmitting of identifying information comprises transmitting a first identifier, associated with the memory unit, a second identifier, associated with the terminal and the first hash value via the mobile communication system to said software provider,

receiving, from the software provider, a data block comprising a digital signature and further data associated with the memory unit and the terminal,

analyzing the received data block, comprising verification of the digital signature and comparison of said further data with said first and second identifiers, and storing the received data block comprising the digital signature, thereby providing a reference value for use during integrity checking of said software module.

22. (Currently Amended)~~Apparatus~~An apparatus, comprising:

a device for enabling integrity checking of a software module to be used in a mobile communication terminal, said terminal capable of communicating in a mobile communication system, said software module already stored on a removable memory unit connected to the terminal and ready for use except, before allowing the software module to take control of the terminal, the terminal communicates via the mobile communication system with a software provider, said device ~~including~~including:

a transmitter for transmitting identifying information concerning said terminal and said memory unit to said software ~~provider~~ provider; and

a receiver for receiving a digitally signed data block comprising a reference value for use during integrity checking of said software module and allowing the software module to take control of the terminal only if the integrity of the software module properly checks.

23. (Currently Amended) The apparatus of claim 22, further comprising:

a device for hashing the software module, resulting in a first hash value, wherein said transmitting of identifying information comprises transmitting a first identifier, associated with the memory unit, a second identifier, associated with the terminal and the first hash value via the mobile communication system to said software ~~provider,~~provider;

a device for receiving, from the software provider, a data block comprising a digital signature and further data associated with the memory unit and the ~~terminal,~~ terminal;

a device for analyzing the received data block, comprising verification of the digital signature and comparison of said further data with said first and second ~~identifiers,~~identifiers; and a device for storing the received data block comprising the digital signature, thereby providing a reference value for use during integrity checking of said software module.